Distributed Security Architectures

Second Quarter 2002 Progress Report

Covers work done Jan through March, 2002

Personnel:

Staff: Mary Thompson, Srilekha Mudumbai, Abdelilah Essiari

Students: Willie Chin

Standalone Server

Added code to the server to handle certificate chains containing both CA certificates and Globus proxy certificates. The chain can be queried to return the name of the end-entity certificate, i.e. the proxy names are ignored.

Implemented an insecure version of the protocol in addition to the secure one, to allow thin clients running on the same host as the server, to perform access checks without needing support SSL communications or cryptographic functions. Made a version of this interface that is callable from C in addition to C++. This API is used by the Globus Job-manager to make callouts to Akenti to check access.

Akenti Server using SOAP protocol

Installed and tested Apache Java SOAP toolkit (http://xml.apache.org/axis/) to gain experience with SOAP communications. Installed gSOAP C++ toolkit (http://www.cs.fsu.edu/~engelen/soap.html) and tested SOAP communication over both http and tcp/ip directly. This is groundwork towards building an Akenti standalone server talking SOAP. Upon our request, the gSOAP group have a new version that supports SOAP over ssl using openSSL.

Akenti Server using Globus I/O

The wrappers needed to integrate globus i/o with Akenti have been written Have a C++ workaround for globus i/o communication. Still working on testing the compatibility between C clients and C++ servers. Expecting input from the globus group regarding their Globus i/o usage.

Certificate Generators

Finished all the XML reading and writing methods for all the certificates and elements. Developed and tested more flexible gui components that allow the user to create, edit, and remove policy elements. Followed the hierarchical structure of the policy certificates in choosing values to prompt with. Tested the certificates created by the new generator code with the Akenti policy engine. Investigated Drag N Drop capabilities that would simplify he use of generators.

Compiled under RedHat Linux

Fixed a few things to make the code compile under RedHat 6.2 as well as RedHat 7.

Code Distribution

.Installed the Akenti sources and supporting packages on machines at Argonne National Lab and the Princton Plasma Physics Lab to be used to control access for a Physics code.

Collaboration with the Secure and Reliable Group Communication project

Investigated policies that would be required by the Secure Group Layer. There are two kinds of security policies needed for secure group communication. One is access policy to determine who can join a group, and the second is the security parameters for running the group, e.g. requirements for rekeying, key strength, message integrity, confidentially and/or authentication.

Access control can be handled by our current policy model. Akenti already provides pre-approval function by allowing a user to request a capability certificate that grants the right to join the group. This certificate can be presented along with the user's authenticated identity to the group controller at the time of the join request. The group controller can then base its access decision on just these two credentials rather than having to call out to the Akenti server. The speed of the access decision is important, since the group controller may need to limit the group communication while allowing a new member to join.

The group parameter policies provide the group controller with the information it needs configure the group and provide members a way to ensure that the group's policy is acceptable before they join. These policies may be treated as a set of run-time constraints that would be returned to the requester for evaluation.

Publications:

A paper on "Authorization Policy in a PKI Environment", M. Thompson, S, Mudumbai, A. Essiari, W. Chin was accepted for the NIST First Annual PKI Workshop, Apr 24-25, 2002.